U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice

Research Report

The Appropriate and Effective Use of Security Technologies in U.S. Schools

A Guide for Schools and Law Enforcement Agencies

U.S. Department of Justice
National Institute of Justice

U.S. Department of Education
Safe and Drug-Free Schools Program

U.S. Department of Energy
Sandia National Laboratories

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

Janet Reno
Attorney General

Raymond C. Fisher
Associate Attorney General

Laurie Robinson
Assistant Attorney General

Noël Brennan
Deputy Assistant Attorney General

Jeremy Travis
Director, National Institute of Justice

Office of Justice Programs
World Wide Web Site
http://www.ojp.usdoj.gov

National Institute of Justice
World Wide Web Site
http://www.ojp.usdoj.gov/nij

The Appropriate and Effective Use of Security Technologies in U.S. Schools

A Guide for Schools and Law Enforcement Agencies

Mary W. Green
Sandia National Laboratories
September 1999

NCJ 178265

National Institute of Justice
Jeremy Travis
Director

Raymond Downs
Program Monitor

This project was supported under award number 97–IJ–R–072 from the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Foreword

Creating safe schools is the responsibility of the entire community in which a school or school system resides, but responsibility for maintaining them on a day-to-day basis lies principally with school administrators and, to a lesser extent, the local law enforcement agency. To assist schools in this task, the U.S. Department of Education and the U.S. Department of Justice have sponsored, often jointly, both research and demonstration programs to collect data and test useful new ideas that will expand understanding of school violence and disorder and lead to new programs to reduce these problems.

This document provides basic guidelines to law enforcement agencies and school administrators and encourages their collaboration as they decide what, if any, security technologies should be considered as they develop safe school strategies. In the wake of recent high-profile school tragedies with multiple homicides, many of this Nation's communities have urged their school districts to incorporate security technology into their safety programs. This guide should help schools, in concert with their law enforcement partners, analyze their vulnerability to violence, theft, and vandalism, and suggest possible technologies to address these problems in an effective manner. This guide describes existing commercially available technologies and urges thoughtful consideration of not only the potential safety benefits that may accrue from their use but also the costs that schools may incur for capital investments, site modifications, additional staffing, training, and equipment maintenance and repair.

Topic areas included in this guide are: security concepts and operational issues, video surveillance, weapons detection devices (walk-through and hand-held metal detectors and x-ray baggage scanners), entry controls, and duress alarms.

Though this document does not replace the use of appropriate expert advice or provide detailed instructions on installing equipment or making cost estimates, it does offer practical guidance that should enable schools and law enforcement agencies to make better informed decisions on security technology.

Safety and security technology can only be one tool in a comprehensive program that each school must develop to create a safe learning environment that is perceived to be safe by all students and staff.

Jeremy Travis
Director, National Institute of Justice
U.S. Department of Justice

Bill Modzeleski
Director, Safe and Drug-Free Schools Program
U. S. Department of Education

Preface

A team of security specialists from the Security Systems and Technologies Center at Sandia National Laboratories first talked with local schools in 1991. It was our intent to share what we had learned about the strengths and weaknesses of security technologies through our work with the U.S. Department of Energy (DOE) in many public schools.

After visiting some 120-plus schools across the country, completing our DOE-funded work to improve security at Belen High School in New Mexico and performing additional school security work for the National Institutes of Justice (NIJ), we have learned that school security, like security for other applications, is not simple and straightforward. We have learned a lot about the unique aspects of school security from the many students, parents, and school and law enforcement personnel we met during the course of our work. At any particular school, security is the product of funding, facilities, building age, building layout, administrators, teachers, parents, kids, personalities, campus order, security personnel, procedures, the neighborhood, policies, the school board, local law enforcement, fire codes, local government, politics, and reputation. No two schools will have identical and successful security programs—hence, a security solution for one school cannot just be replicated at other schools with complete success.

What did become clear after working with more than 100 schools during the past 7 years is that school administrators need a good information resource on technologies for physical security problems. This guidebook, *The Appropriate and Effective Use of Security Technologies in U.S. Schools,* is anticipated to be the first in a series of manuals designed and written for use by school administrators and law enforcement agencies. The goals of these documents are to provide nontechnical, nonvendor-specific information on:

- The kinds of security products available on the market.
- The strengths and weaknesses of these products and their expected effectiveness in a school environment.
- The costs of these products, including installation, long-term operational and maintenance expenses, manpower, and training.
- Requirements to include in Requests For Quotes (RFQs) to get a good product for an application.
- Legal issues that may need to be addressed.

Although security products can certainly have many different applications, this document covers products that can be applicable to some of the issues of violence in schools: video surveillance, weapon detection, entry control, and duress alarms. Future volumes are expected to cover issues and products such as bomb threats and explosives detection; drug residue and drug vapor detection; drug use detection; alcohol use detection; interior and exterior intrusion detection sensors; alarm communications; antigraffiti sealers; false fire alarm pulls; glass-break sensors; two-way radios; fencing; antitheft property marking; doors, locks, and key control; Crime Prevention Through Environmental Design (CPTED) principles; and parking lot safety. Most of the issues and philosophies covered in these manuals are geared toward middle schools and high schools, but elementary schools will likely find several of the technologies to have possible applications at their facilities.

Although this document addresses nontechnology measures that we felt were important for the completeness

of the topic, there are many good resources and references available that address these people/policy/procedure/program issues much better. See the Resources section at the back of this book.

Feedback from law enforcement agencies, schools, and product manufacturers/vendors is welcome, especially regarding any oversights or errors on our part. This guidebook is intended to provide an overview of security technology product areas that might be appropriate and affordable for school applications. Appropriate corrections or additions will be included in future updates. (We apologize if our cost estimates for hardware do not reflect current pricing; this document was written more than a year before actual publication.)

I would like to extend our deep appreciation to the many schools who have allowed us to visit them and to assess the security vulnerabilities of their facilities and operations (and to take photos of the good things on their campuses, as well as the bad). I never failed to learn something new at every school we have visited. I found there to be many great schools in this country, with very motivated and hard-working administrators giving 110 percent of their energies to keep their students safe. I was humbled by the intense and stressful hours they worked and the ultimate importance of their jobs.

My thanks to the National Institute of Justice (NIJ) for providing the funding to conduct the research that allowed me to prepare this guidebook. I hope that we have met the high standards NIJ has set for providing the best that science and technologies have to offer in fighting crime in the United States. I owe special gratitude to Dennis Miyoshi, Director of Sandia's Security Systems and Technologies Center; Dennis has always been an advocate for schools and was the greatest ally in accomplishing Sandia's school security work.

Information regarding the availability and ordering process for these manuals and any updates may be obtained at the NIJ Web site: *www.ojp.usdoj.gov/nij;* the Justice Technology Information Network (JUSTNET): *www.nlectc.org;* or by calling 1–800–248–2742.

I would be interested in hearing from readers regarding their successes, as well as their failures, in dealing with school security technology issues.

Mary W. Green
mgreen@sandia.gov
Sandia National Laboratories
Mail Stop 0782
P.O. Box 5800
Albuquerque, NM 87185

Since 1941, Sandia National Laboratories has been a U.S. Department of Energy facility whose primary mission is providing engineering support for the U.S. nuclear weapons program. For the past 30 years, the Security Technologies and Research Division at Sandia has been the principal provider of research, design, development, and testing of leading-edge technologies to solve physical security problems at high-risk U.S. facilities.

Today, the Sandia facility in Albuquerque, New Mexico, employs more than 8,000 scientists, engineers, mathematicians, technicians, and support personnel to provide service in the national interest. More than 150 of these personnel are dedicated solely to research and development of security technologies.

Acknowledgments

Written by:	Mary W. Green, Sandia National Laboratories, Albuquerque, New Mexico
Original art work by:	Steven Scatliffe, Tech Reps, Inc., Albuquerque, New Mexico
Photos by:	George Wagner, Sandia National Laboratories, Albuquerque, New Mexico Steven Scatliffe, Tech Reps, Inc., Albuquerque, New Mexico
Document preparation:	Rosanne C. Rohac, Tech Reps, Inc., Albuquerque, New Mexico Elaine Perea, Tech Reps, Inc., Albuquerque, New Mexico
Additional contributors:	Janet Ahrens, Sandia National Laboratories, Albuquerque, New Mexico Tim Malone, Sandia National Laboratories, Albuquerque, New Mexico Dale Murray, Sandia National Laboratories, Albuquerque, New Mexico Charles Ringler, Sandia National Laboratories, Albuquerque, New Mexico George Wagner, Sandia National Laboratories, Albuquerque, New Mexico Fred Wolfenbarger, Sandia National Laboratories, Albuquerque, New Mexico
Library research:	Kay Kelly, BEI, Albuquerque, New Mexico
Reviewers:	Raymond Downs, Program Manager, National Institute of Justice William Modzeleski, Director, Safe and Drug-Free Schools Program, U.S. Department of Education Joe N. Anderson, Director of School Safety and Security, Metropolitan Nashville Public Schools Michael S. Ganio, Sr. Manager, Security Services, Orange County Public Schools John J. McLees, Executive Director, Philadelphia Office for School Safety Tom Hall, School Police Chief, San Diego Unified School District Kenneth Trump, President and CEO, National School Safety and Security Services Gary Underwood, Chief, San Bernardino Police, School Safety Department Paul Schultz, Chief of Police, LaVista Police, LaVista, Nebraska Ronald Sloan, Chief of Police, Arvada Police Department, Arvada, Colorado John C. Martinez, Deputy Chief, Dallas Police Department J.M. Hutt, Sergeant Arapahoe County Sheriff's Office, Englewood, Colorado Tod Schneider, Crime Prevention Specialist, Police Services Division, Eugene, Oregon Ed Hardy, Chief, Special Investigative Unit, Broward County School District, Sunrise, Florida Donovon Collins, Chief, Dallas Independent School District Police Mel Seo, Auxiliary Service Specialist, Hawaii Department of Education Jack Lazzarotto, Director, Police Services, Clark County School District, Las Vegas, Nevada Charles Clark, Director, Security Emergency Preparedness, Long Beach Unified School District Wesley Mitchell, Chief, Los Angeles School Police Sharon O'Connor, Tech Reps, Inc., Albuquerque, New Mexico

Contents

Foreword iii

Preface v

Acknowledgments vii

Chapter I The Big Picture: Security Concepts and Operational Issues 1

Chapter II Video Surveillance 23

A. Video cameras 23
1. Why video cameras? 23
2. Why NOT video cameras? 25
3. Good applications versus poor applications 25
4. To monitor or not to monitor 30
5. Color versus black-and-white cameras 32
6. Fixed versus pan-tilt-zoom cameras 32
7. Hardwired versus wireless systems 33
8. A more technical discussion of formats, resolution, pixels, lenses, and field of view 38
9. Camera housings 45
10. Placement and mounting 48
11. Lighting requirements and nighttime applications 49
12. Covert cameras 51
13. Maintenance and expected lifespan 53
14. Price ranges 53
15. Going out on bid for equipment and system maintenance contracts 53
16. Signage for use of cameras on school grounds 56
17. Legal aspects of the use of video cameras in schools 57

B. Video recording equipment 57
1. VCRs: the weak link 57
2. Multiplexers 58
3. Time-lapse recorders 61
4. Event recorders 62
5. Digital recorders 62

Chapter III Metal Detection 65

A. Walk-through metal detectors for personnel 65
1. Do metal detectors really work?—The basics 65
2. Space requirements and layout 66
3. Throughput 70
4. Hardware costs and manpower costs 71
5. Procedures for the operator 74
6. Instructions for the scannee 76
7. False alarms 76
8. Sources of interference 78
9. Acceptance testing and performance testing 81
10. Maintenance and expected lifespan 82
11. Working with the vendor 82

B. Hand-held scanners for personnel 84
1. The name of the game: Policies and procedures 86
2. Space requirements 86
3. Throughput 86
4. Hardware costs and manpower costs 87
5. Procedures for the operator 87
6. Instructions for the scannee 90
7. Maintenance and expected lifespan 92
8. Working with the vendor 92

C. X-ray baggage scanners 92
1. Safety concerns 92
2. Setup and space requirements 93
3. Throughput 93
4. Hardware costs and manpower costs 95
5. Procedures for the operator 96
6. Instructions for the scannee 98
7. Acceptance testing and performance testing 99
8. Maintenance and expected lifespan 99
9. Working with the vendor 101

Chapter IV Entry-Control Technologies 103

A. Limiting entry/exit points 103

B. Entry-control approaches 106
1. WHO lets you in 106
2. What you HAVE 106
3. What you KNOW 108
4. Who you ARE 110

Chapter V Duress Alarm Devices and Their Role in Crisis Management 113

Resources: Books, Publications, Web Sites, and Conferences 121

Pearl High School, Pearl, Mississippi